モデル検査ツール PRISM によるネットワーク構成図上でのランサムウェア攻撃のモデル化

1240339　田上　和真　【 ソフトウェア検証・解析学研究室 】

1　はじめに

ランサムウェアとは暗号化によりシステムやファイルを使用不能にし，その復旧と引き換えに身代金を要求する攻撃のことである．近年企業・団体へのランサムウェア被害件数が増加してきている．

Skeoch [1] は，ランサムウェア攻撃の過程を部分観測マルコフ決定過程としてモデル化し，1 台の感染確率等のパラメータによる違いを予測できるようにした．しかし，近年増加しつつある侵入型ランサムウェア攻撃のモデルとしては精密さに欠ける．そこで本研究では [1] のモデルを改良した確率モデルを提案し，本モデルによりより精密な分析が可能であることを示す．

2　提案するモデル

先行研究のモデルに改良を加えたモデルを図 1 に示す．主に以下の 4 点が先行モデルと異なる．(1) 先行モデルでは，身代金の支払いによって確実に完全に修復すると仮定していたが，現実では必ずしもそうとは限らない．提案モデルでは，身代金の支払いによって修復するかどうかは確率的とした．(2) 先行モデルでは，感染した後潜伏し感染範囲を広げるという侵入型ランサムウェア攻撃の過程を再現できていなかった．提案モデルでは，潜伏を表す状態を追加してこの再現を図った．(3) 先行モデルでは考慮されていなかった，潜伏状態での危険検知による遮断アクションを追加した．(4) 先行モデル・提案モデルとも，攻撃対象となるコンピュータが複数あり，それぞれ重要度 高・中・低に分類されていると仮定している．先行モデルではそれらの機器間のネットワークの形状を考慮していなかった．提案モデルでは，確率的遷移モデルに加えてネットワーク構造図も考慮して，感染拡大過程を予測するモデルとした．

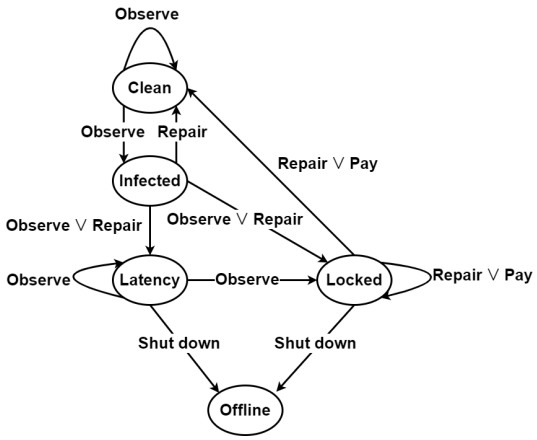

図 1　提案モデルの確率的遷移構造

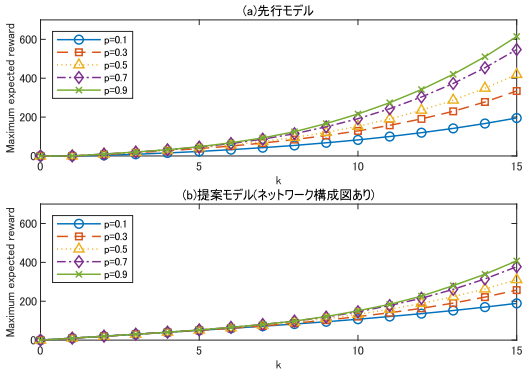

図 2　低重要度のコンピュータへの感染率の変化が与えるコスト累積への影響

3　シミュレーション結果

先行モデル・提案モデルに各状態遷移確率を設定することで，以下のような指標を計算することができる．

- 機密性：重要度が高・中のコンピュータが感染もロックもされない確率
- 完全性：全コンピュータが感染しない確率
- 可用性：全コンピュータがロックされない確率
- コスト：時間経過に伴う費用

例えば 図 2 (a)・(b) は，先行モデルと提案モデルを使って計算したコストの値を示すグラフである．重要度高・中・低のコンピュータをそれぞれ 1 台・1 台・8 台として計算している．横軸は経過時間を表す．各折れ線は低重要度のコンピュータの感染確率 p に対応している．

これらの図から，モデルの違いによりコストの推定結果が変化することが分かる．先行モデルでは調節できない箇所を提案モデルでは調節できるようになっており，実際の状況により近づけてシミュレーションを行えると考えられる．

提案モデルにおいてネットワーク構成図を考慮する場合としない場合を比較すると，考慮しない場合は先行モデルと異なる特徴を持つ推定結果が得られ，考慮する方が機密性・完全性・可用性は高くコストは低いと推定する傾向があった．ネットワーク構成図を考慮しないモデルは「どのような経路でも感染が広がる」という悲観的モデルであり，感染経路が限定される状況の場合は提案モデルの方が現実に合うと考えられる．

参考文献

[1] H.R.K. Skeoch, “Modelling Ransomware Attacks using POMDPs”, WEIS 2022.